IN THE CLAIMS

Please cancel claims 4 and 8 without prejudice or disclaimer of their (its) subject matter, amend claims 1-3, 5-7, and 9-17 based on the pages 23 to 28 in the English translation corresponding to the claim section, pages 46 to 52, of the original specification, and add new claims 18 to 40, to read as follows:

---

1. (Amended) A system for preventing an illegal copy of digital content, said system receiving and decrypting encrypted digital content and reproducing the digital content, comprising:

a certificate authority for generating manufacturer key information and generating first key information for giving an authorization to supply said encrypted digital content;

a portable terminal supplier supplying a portable terminal, said portable terminal supplier outputting a first registration request signal to said certificate authority and receiving the manufacturer key information generated by said certificate authority in accordance with the first registration request signal, said portable terminal supplier imbedding the manufacturer key information in said portable terminal;

a content supplier transmitting a second registration request signal to the certificate authority, said certificate authority and said content supplier sharing a first secret channel, said content supplier receiving and storing said first key information from the certificate authority through said first secret channel for supplying said encrypted digital content, said content supplier generating and outputting second key information for giving an authorization to receive and reproduce said encrypted digital content;

a personal computer outputting a third registration request signal to the content supplier for obtaining said second key information, said personal computer having public key information of said certificate authority, said personal computer and said content supplier sharing a second secret channel, said personal computer verifying said first key information inputted from the content supplier by using said public key information of said certificate authority and receiving the second key information through said second secret channel, said personal computer receiving said encrypted digital content through said second secret channel; and

said portable terminal manufactured by said portable terminal supplier for reproducing said digital content, said portable terminal transferring the imbedded manufacturer key information to said content supplier through said personal computer to be verified by said content supplier, said portable terminal and said personal computer sharing a third secret channel for transferring said encrypted digital content between said portable terminal and said personal computer.

2. (Amended) The system as claimed in claim 1, wherein the certificate authority generates a first channel key shared with the content supplier to form said first secret channel, the first key information is encoded by said first channel key and then transferred to said content supplier, and said content supplier decodes the encoded first key information by said first channel key.

3. (Amended) The system as claimed in claim 1, wherein the content supplier generates a second channel key shared with the personal computer to form said second secret channel, and the second key information is encoded by said second channel key, and then transferred to said personal

computer.

5. (Amended) A system for preventing an illegal copy of digital content, comprising:

a certificate authority for generating manufacturer key information comprising a manufacturer key and a manufacturer key data in response to a first registration request signal inputted from an external source, generating first key information for giving an authorization to supply said digital content, said certificate authority generating a token to make an information table, said information table comprising a first table containing the manufacturer key data, the manufacturer key, and an identifier corresponding to the manufacturer key, and a second table containing said identifier, token information encrypted by said manufacturer key, and said token;

a content supplier transmitting a second registration request signal to the certificate authority for supplying said digital content, said certificate authority and said content supplier sharing a first secret channel, said content supplier receiving and storing said first key information and said second table from the certificate authority through said first secret channel, said content supplier generating second key information;

first content output means for outputting the digital content, said first content output means sending a third registration request signal to the content supplier for downloading said digital content from said content supplier, said first content output means having public key information of said certificate authority, said first content output means and said content supplier sharing a second secret channel, said first content output means verifying said first key information inputted from the content supplier by using said public key information of said certificate authority and receiving the second

key information through said second secret channel, said first content output means extracting the manufacturer key information from said second table, and encoding and outputting the manufacturer key information; and

said second content output means for recording and reproducing said digital content, said second content output means storing the manufacturer key information, said second output means transferring said manufacturer key information to said content supplier through said first content output means to be verified by said content supplier, said second content output means receiving said manufacturer key information of said second table from said first content output means to decide if the manufacturer key is authenticated, said second content output means and said first content output means sharing a third secret channel for transferring said digital content between said second content output means and said first content output means.

6. (Amended) The system claimed in claim 5, wherein a content storage means is further included in at least one of said second content output means and said first content output means, and said content storage means stores said digital content.

7. (Amended) The system claimed in claim 5, wherein the certificate authority generates a first channel key shared with the content supplier to form said first secret channel, the first key information is encoded by said first channel key and then transferred to said content supplier, and said content supplier decodes the encoded first key information by said first channel key.

9. (Amended) The system claimed in claim 5, wherein the content supplier generates a second channel key shared with the first content output means to form said second secret channel, and the second key information is encoded by the second channel key, and then transferred to said first content output means.

A3 cont

10. (Amended) The system claimed in claim 5, wherein the token is randomly generated by the certificate authority.

11. (Amended) The system claimed in claim 7, wherein the first content output means generates a third channel key shared with the second content output means to form said third secret channel, and the first content output means encodes the third channel key with said token inputted from the content supplier and transmits the third channel key to the second content output means.

12. (Amended) The system claimed in claim 11, the second content output means decodes the encoded token transmitted from the first content output means by using the stored manufacturer key, decodes and stores the third channel key by using said token.

13. (Amended) The system claimed in claim 11, further comprised of:

said first content output means including a database which has reproduction data of the digital content downloaded from the content supplier, said first content output means encoding the database by using the third channel key for storage, interpreting the reproduction data of the digital

content by using the third channel key to thereby judge if an illegal copy of the digital content is performed; and

said second content output means receiving said reproduction data from said first content output means, updating the reproduction data whenever any content downloading or uploading session between said first content output means and said second content output means occurs, and transmitting the updated reproduction data of the digital content to the first content output means.

14. (Amended) The system claimed in claim 13, wherein the database is separated with an identifier data area of the digital content, an updated token data area, a data area for a present state of the digital content, and a reproduction control data area, and has the corresponding data.

15. (Amended) The system claimed in claim 14, wherein the data area for the present state of the digital content comprises:

first data indicating that the digital content is downloaded in a copy form from the first content output means to the second content output means;

second data indicating that the digital content is downloaded in a transmission form from the first content output means to the second content output means; and

third data indicating that the digital content is downloaded and uploaded between the first content output means and the second content output means.

16. (Amended) The system claimed in claim 14, wherein the reproduction control data area

of the digital content includes:

fourth data for reproduction times of the digital content;

fifth data for a reproduction expiration period of the digital content; and

sixth data for an amnesty period of the digital content.

17. (Amended) A system for protecting a illegal copy, comprising:

a terminal receiving a physical address of a bad sector of a storage medium, said terminal generating a random number and storing said random number in a spare area of said storage medium, said terminal having a secret channel key, said terminal function-processing said physical address, said random number and said secret channel key to obtain a processed value, said terminal encrypting a header of the digital content by the processed value; and

said storage medium transmitting said physical address of the bad sector, storing said random number as a key value generated from said terminal, storing as a sector data the encrypted digital content and the header of the digital content encrypted by using the processed value.

--18. A system for protecting an illegal copy of digital content, comprising:

a certificate authority for generating manufacturer key information and generating first key information for giving an authorization to supply said digital content;

a terminal supplier supplying a terminal, said terminal supplier outputting a first registration request signal to said certificate authority and receiving the manufacturer key information generated by said certificate authority in accordance with the first registration request signal, said terminal supplier

embedding the manufacturer key information in said terminal;

a content supplier sending a second registration request signal to the certificate authority, said certificate authority and said content supplier sharing a first secret channel, said content supplier receiving and storing said first key information from the certificate authority through said first secret channel for supplying said digital content, said content supplier generating and outputting second key information for giving an authorization to receive and reproduce said digital content from said second key information;

a personal computer sending a third registration request signal to the content supplier for obtaining said second key information, said personal computer having public key information of said certificate authority, said personal computer and said content supplier sharing a second secret channel, said personal computer verifying said first key information inputted from the content supplier by using said public key information of said certificate authority and receiving the second key information through said second secret channel, said personal computer receiving said digital content through said second secret channel;

said terminal manufactured by said terminal supplier for reproducing said digital content and reading a storage medium, said terminal transferring the embedded manufacturer key information to said content supplier through said personal computer to be verified by said content supplier, said terminal and said personal computer sharing a third secret channel for transferring said digital content between said terminal and said personal computer, said terminal receiving and function-processing a physical address of a bad sector of the storage medium, a random number generated and stored in a spare area of said terminal and a secret channel key generated in said terminal to obtain

a processed value, said terminal encrypting a header of the digital content with the processed value; and

said storage medium transmitting said physical address of the bad sector, storing said random number as a key value generated from said terminal, storing as a sector data the encrypted header of the digital content and encrypted header information encrypted by using the result of function processing.

--19. The system claimed in claim 18, wherein the certificate authority generates a first channel key shared with the content supplier to form said first secret channel, the first key information is encoded by said first channel key and then transferred to said content supplier, and said content supplier decodes the encoded first key information by said first channel key, the content supplier generates a second channel key shared with the personal computer to form said second secret channel, and the second key information is encoded by the second channel key, and then transferred to said personal computer, and the personal computer generates a third channel key shared with the terminal to form said third secret channel, and the personal computer encodes the third channel key with said token inputted from the content supplier and transmits the third channel key to the terminal.

--20. The system claimed in claim 19, further comprised of:

said personal computer having a database which comprises reproduction data of the digital content downloaded from the content supplier, the database encoded by using the third channel key,

said personal computer interpreting the digital content by using the third channel key to decide if an illegal copy of the digital content is performed; and

said terminal receiving said reproduction data from said personal computer, updating the reproduction data whenever any content downloading or uploading session between said terminal and said personal computer occurs, and transmitting the updated reproduction data to the personal computer.

a3

--21. The system claimed in claim 20, wherein the database is separated with an identifier data area of the digital content, an updated token data area, and a data area for a present state of the digital content, and a reproduction control data area.

--22. The system claimed in claim 21, wherein the data area for the present state of the digital content includes first data indicating that the digital content is downloaded in a copy form from the personal computer to the terminal. second data indicating that the digital content is downloaded in a transmission form from the personal computer to the terminal, and third data indicating that the digital content is downloaded and uploaded between the personal computer and the terminal, and the reproduction control data area of the digital content includes fourth data for reproduction times of the digital content, fifth data for a reproduction expiration period of the digital content; and sixth data for an amnesty period of the digital content.

--23. A server for preventing an unauthorized copy of digital content, said server comprising:

a first cryptosystem verifying public key information of a content provider by using public key information embedded in said server to check whether said content provider has an authorization to supply said digital content, said server establishing a second secure channel to said content provider to download said digital content from said content provider;

a second cryptosystem encrypting and transfering manufacturer key information embedded in a terminal linked to said server from said terminal to said content provider to be verified by said content provider, said server establishing a third secure channel to said terminal after the validation of the manufacturer key information, said server transfering a token of said content provider to said terminal through said second secure channel and said third secure channel; and

a secure check-in and check-out system for checking a validation of said digital content, said secure check-in and check-out system comprising a right management system having a right management database, wherein information of said digital content corresponding to said right management database is registered to said right management system, said right management database is updated whenever said digital content is downloaded or uploaded between said server and said terminal to check if an unauthorized copy of said digital content is performed.

--24. The server of claim 23, wherein said second secure channel is established by executing a handshaking protocol to get an ephemeral shared key by utilizing Elliptic curve based key exchanging protocol.

--25. The server of claim 23, wherein said third secure channel is established by a third secret

channel key generated in one of said server and said terminal.

--26. The server of claim 25, wherein said right management database comprises reproduction data of said digital content, said server encodes said reproduction data by using said third secure channel key, and said server checks said reproduction data by using said third secure channel key.

--27. The server of claim 25, wherein said right management database comprises an identifier data area of the digital content, an updated token data area, a data area for a present state of the digital content, and a reproduction control data area.

--28. The server of claim 27, wherein the data area for the present state of the digital content comprises:

first data indicating that the digital content is downloaded in a copy form from said server to said terminal;

second data indicating that the digital content is downloaded in a transmission form from said server to said terminal; and

third data indicating that the digital content is downloaded and uploaded between said server and said terminal.

--29. The server of claim 27, wherein the reproduction control data area of the digital content

comprises:

fourth data indicating reproduction times of the digital content;

fifth data indicating a reproduction expiration period of the digital content; and

sixth data indicating an amnesty period of the digital content.

Q3 am4

--30. The server of claim 27, wherein said digital content has a first file format comprises:

a plain header comprising a title identifier, a content description field, and an algorithm identifying field from which said server finds out an encryption algorithm and a secret key of said server;

a secret header comprising a device identifier to be compared with an identifier of said server, an indicator of a source origination of said digital content, a right management field including data to be registered to said right management system, and a content encryption key for recovering said digital content encrypted by said content encryption key; and

a file body comprising said digital content encrypted by using said content encryption key.

--31. The server of claim 30, further comprising:

an applied program interface confirming a validity of an input and extracting first information from said input;

an import control layer receiving said first information from said applied program interface, said import control layer reconstructing said first information into said first file format; and

a terminal interface authenticating said terminal by checking whether said terminal has a

correct identifier and said third secret channel key.

--32. A terminal, comprising:

manufacturer key information embedded in said terminal; and

a symmetric key cryptosystem preventing an unauthorized copy of digital content by responding to reception of said manufacturer key information by a server by establishing a secure registration of said terminal with said server, with said terminal establishing a third secure channel to said server and said terminal receiving a token from said server through said third secure channel to reproduce said digital content provided by said server.

--33. The terminal of claim 32, further comprising:

a public key cryptosystem, wherein said terminal verifies public key information of said server by using public key information embedded in said terminal to check whether said server has an authorization to download said digital content to said terminal.

--34. The terminal of claim 32, wherein said terminal generates update token data whenever said digital content is downloaded or uploaded between said terminal and said server to check if an unauthorized copy of said digital content is performed.

--35. The terminal of claim 34, wherein said third secure channel is established by a third secret channel key.

--36. The terminal of claim 35, wherein said update token data are encoded and decoded by said third secret channel key.

--37. The terminal of claim 32, wherein said digital content has a first file format comprising:

a plain header comprising a title identifier, a content description field, and an algorithm identifying field;

a secret header comprising a device identifier, an indicator of a source origination of said digital content, a right management field, and a content encryption key for recovering said digital content encrypted by said content encryption key; and

a file body comprising said digital content encrypted by said content encryption key.

--38. The terminal of claim 37, wherein said terminal is able to write said digital content encrypted by said content encryption key on a storage medium, recover said secret header, and reencrypt said digital content by using an unique identifier in said storage medium, and, if said storage medium does not have said unique identifier in said storage medium, said terminal is able to write said digital content encrypted by said content encryption key on said storage medium, recover said secret header, reencrypt said digital content by using a randomly generated key, and encrypt and write said randomly generated key on a hidden area of said storage medium by using a common secret key embedded in said terminal.

--39. The terminal of claim 37, wherein said terminal has an import control layer to convert an analog input to said digital content having said first file format.

--40. The terminal of claim 38, wherein said unique identifier is a physical address of a bad sector of said storage medium, said terminal has a random number generator to generate a random number and stores said random number in a spare area of said storage medium, and said terminal has a function-processor function-processing said physical address, said random number and said third secure channel key to obtain a processed value, and said terminal encrypts said digital content with the processed value.